Quick Start Guide

3Com® Embedded Firewall

http://www.3com.com/
http://www.3com.com/registration/frontpg.pl

09-2110-002
Published November 2002

3Com Corporation ■ 5400 Bayfront Plaza ■ Santa Clara, California ■ 95052-8145 ■ U.S.A.

3Com, EtherCD, and EtherLink are registered trademarks and the 3Com logo is a trademark of 3Com Corporation. Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other company and product names may be trademarks of the respective companies with which they are associated.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as “Commercial Computer Software” as defined in DFARS 252.227-7014 (June 1995) or as a “commercial item” as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com’s standard commercial license for the software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this user guide.

EXPORT RESTRICTIONS

This 3Com product and/or software contains encryption and may require U.S. and/or local government authorization prior to export or import to another country.

Contents

Quick Start Guide

This quick start guide assists you in installing and configuring a basic 3Com Embedded Firewall (EFW) system. You can use this basic EFW system as a starting point and tailor the system to your organization's security needs.

This guide provides a stationary EFW device installation example and a roaming EFW device installation example. All new users should complete the stationary installation as it provides an introduction to basic system concepts. A stationary EFW device is an EFW device in a desktop or server host. Such devices remain in one location and have one policy. A roaming EFW device is a laptop (mobile) card that moves between the enterprise network and locations outside the enterprise network. A roaming EFW device has two policies, a local and a remote policy.

Any EFW system installation begins with the installation of the EFW Policy Server and Management Console software. Using the Management Console you will:

- Set up the license-activation keys that enable all of the EFW functionality
- Create a backup of the Policy Server (for recovery)
- Create a policy
- Install an EFW device
- Change the policy for an EFW device
- Test policy enforcement

Experienced EFW users may skip to the roaming EFW device installation example, which demonstrates new functionality available in this release. Novice users may continue on with this exercise as desired after the stationary EFW device installation. For roaming EFW device installation you will:

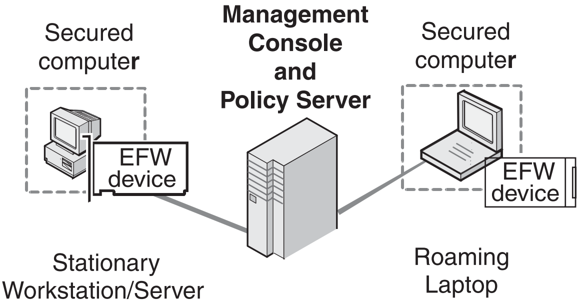
- Create local and remote policies
- Configure the system to determine the roaming device's location
- Install an EFW device
- Test local and remote policy enforcement

After completing the steps in this guide, you will have a basic EFW system setup that includes:

- An operational Policy Server and Management Console
- Two embedded firewall (EFW) devices
- An understanding of how to import and create policies

- An understanding of how to configure stationary EFW devices with one policy (for desktops and servers) and/or roaming EFW devices with two policies (for laptops)
- An understanding of how to change the policy for an EFW device

The following is an illustration of the basic EFW system created using this guide:



The final section in this guide points you to key sections in the *3Com Embedded Firewall Administration Guide* that provide detailed information for expanding your EFW system to best suit your security needs. This document is found in the docs folder of the 3Com Embedded Firewall CD.

NOTE: This guide provides one basic example of EFW installation, for an understanding of all installation methods, refer to the *3Com Embedded Firewall Administration Guide*.

What You Will Need

Before you install the EFW software, you will need:

1. A computer to host the Policy Server and Management Console that meets the following requirements:
   - Operating system: Microsoft Windows 2000 (Server and Advanced Server), NT Server 4-SP4 or higher. The following will operate as demonstration systems for evaluation purposes only, a warning will appear during installation explaining this: NT Workstation, Windows 2000 Professional and XP (Home Edition and Professional Edition)
   - CPU: 600 Mhz or higher (recommended)
   - RAM: 128 MB
   - Disk space 150 MB

- Monitor/video: 256 colors or higher, screen area set to 600 x 800 or higher
- System with a static IP address

2 A computer to host a stationary EFW device that meets the following requirements:

- Operating system: Microsoft Windows 98 SE, 2000 (Server, Advanced Server, or Professional), NT 4-SP4 or higher, or XP (Home or Professional Edition)
- CPU: No minimum requirement
- RAM: 16 MB
- Web browser with access to the Internet (for testing purposes)
- 3Com Firewall Card (FWC) that supports EFW, with factory drivers installed and operational in the network. Any card listed in Chapter 1 of the *3Com Embedded Firewall Administration Guide* including the mobile cards, can be used for the stationary example.

3 A computer to host a roaming EFW device that meets the following requirements:

- A laptop with a VPN client, operational for remote VPN access to your enterprise LAN, through the network card. The VPN connection must go through the EFW device, not a DSL or Cable modem that connects through a USB port or an integrated network interface card.
- All the requirements listed above for the computer hosting the stationary EFW device
- The EFW device in the laptop is a 3Com Firewall PC card with model number 3CRFW102 or 3CRFW103

4 Network connectivity between the three systems listed above. We refer to the network as your “enterprise LAN.”

5 Capability to move file folders larger than a diskette from the Policy Server computer to the others (for example, a zip drive on each system, file compression software such as WinZip, and FTP on each system, a shared drive, etc.)

6 One 3.5” diskette for creating the Policy Server backup diskette

7 Administrative privileges on all systems (required to install and run EFW software as instructed here)

As an option, you can do all exercises in this guide with a single laptop (meeting the specifications above) plus a computer to host the Policy Server and Management Console. However, you will need to perform an uninstall and reinstall as instructed.

You should also become familiar with the *3Com Embedded Firewall Administration Guide*. If you encounter problems during installation, refer to Appendix B, “Troubleshooting,” in that guide. It offers a list of common problems you may encounter and offers suggestions for solving these problems. If you have any further questions, contact 3Com technical support as described in the administration guide.

Installing EFW Policy Server and Management Console Software

The steps below provide instructions for installing a Policy Server and Management Console on a single system using the Typical installation method.

1. Insert the 3Com Embedded Firewall CD in the appropriate drive; the Installation wizard launches automatically, and a Welcome window appears.
2. Click *Next*. The License Agreement window appears. Read the terms of the license agreement, and select *I accept the terms in the license agreement*.
3. Click *Next*. The Customer Information window appears. Type your user name and organization name in the appropriate fields.
4. Click *Next*. The Installation Type window appears.
5. Select *Typical Centralized Management*. This selection installs the Policy Server software and Management Console software.
6. Click *Next*. In the EFW Domain Association window, select *Create a new EFW domain*. An EFW domain is a collection of Policy Server and EFW device components that can share EFW-related data. EFW domains are not related to Windows domains.
7. Click *Next*. The Ready to Install the Program window appears.
8. Click *Install*. The Installation wizard installs the features you selected. A status bar appears, allowing you to monitor the installation progress.
9. When the Installation wizard is complete, the InstallShield Wizard Completed window appears.
10. Click *Finish* to complete the installation process.

11 When the window appears asking if you want to start the Policy Server now, click *Yes*.

12 Remove the CD from the drive.

Initializing the Policy Server

The first time you start the Policy Server, the Join Existing EFW Domain or Create EFW Domain window appears. Follow the steps below.

1 Select the host name or IP address for the new Policy Server from the list displayed.

If all EFW devices and Policy Server hosts in your EFW domain will reside on one network, select the host name.

Otherwise, select an IP address such that:

- the hosts for the EFW devices that will belong to this EFW domain can resolve this address
- traffic originating at the Policy Server machine and going to the EFW devices in this domain is routed through the network card on the Policy Server machine corresponding to this address.

In most cases only one IP address is offered on this screen.

NOTE: Under some network configurations, you may successfully select the host name option here, even if your EFW domain is spread across several networks. If you are interested in examining this option in detail now, refer to the section "Joining a New Policy Server to a Domain" in the *3Com Embedded Firewall Administration Guide.*

2 Select *Confirm Create New Domain*.

3 Enter a domain name in the Domain Name field.

The EFW domain name is used only as a reference to assist you in identifying a particular EFW domain, if multiple EFW domains are created.

4 Click *OK*. A Policy Server Startup window appears, displaying the status of the various Policy Server components.

When *Policy Server Initialized* appears at the bottom of the window, the Policy Server is fully operational. To close this window, click the X in the upper right corner of the window. (This window is informational only and may be left open or closed at any time without affecting the Policy Server.)

NOTE: After first start-up, the Policy Server automatically starts upon system reboot.

Starting the Management Console and Connecting to the Policy Server

The Management Console is the administrative interface to the Policy Server. You can configure the system and view data using the Management Console. To start the Management Console, follow the steps below.

1. From the Windows Start menu, select *Programs* -> *3Com Embedded Firewall Management*. One of the following two options appears:
   - *3Com Embedded Firewall Management Console*—If this option appears, select it to open the 3Com Embedded Firewall Login window.
   - *3Com MMC Embedded Firewall Management Console*—If this option appears, select it to open the 3Com MMC Embedded Firewall Management Console, and then double-click *Embedded Firewall Management Console*. The 3Com Embedded Firewall Login window appears.
2. Enter your EFW login name and password in the appropriate fields.
   The default EFW login and password (case sensitive) for a new system are as follows:
   - Login: *admin*
   - Password: *admin*
3. Select the Policy Server that you just created from the Policy Server list.
4. Click *Connect*. The Embedded Firewall Management Console window appears, and the Policy Server to which you are connected is listed in the Server tab of the tree-view frame.

NOTE: An information window appears the first time you connect to the Management Console, notifying you that no Policy Server or EFW device licenses currently exist. You will learn how to add license-activation keys in the following section. Click *OK* to close the License Warning window.

Setting up License-activation Keys

License-activation key numbers are provided with the EFW software. The first time you log in to the system, you must enter these keys to enable all of the EFW functionality. Two types of licenses exist, Policy Server licenses and EFW device licenses. To complete the steps in this guide, you need to add an activation key for the Policy Server you installed. If you are using EFW devices that are pre-licensed you do not need separate device license keys. Otherwise you will need an EFW device license for each EFW device you install. See the *3Com Embedded Firewall Administration Guide* for a list of pre-licensed firewall cards. For more information on license-activation keys, refer to the section “Licensing Overview” in the *3Com Embedded Firewall Administration Guide.*

To add the activation keys, follow the steps below.

1. In the Management Console *Tools* menu, select *License Manager*.
   The License Summary window appears.

2. Click *Add Keys*. The Add Activation Key window appears. Enter the activation key and click *Add* for each activation key that you want to add.

3. When you have finished adding activation keys, click *Close* to close the Add Activation Key window.

4. Click *Close* to close the License Summary window. All EFW system functionality is now available.

Creating and Retaining a Backup

Communication is encrypted between EFW devices and the Policy Server, between the Management Console and the Policy Server, and between Policy Servers. Policy Servers identify themselves to each other, to the Management Console, and to their EFW devices (firewall cards) using two public/private key pairs generated upon creation of a new EFW domain.

Immediately after installing your first Policy Server in an EFW domain, it is critical to make a backup copy of the Policy Server database, which contains cryptographic information that will be required to communicate with devices in the domain. Save this data indefinitely in a safe, secure location.

In the unlikely event of a disaster, such as a disk crash on all of your Policy Server machines and a simultaneous loss of all disk backups for these machines, this backup diskette allows you to “clone” your policy server and regain management control of your EFW devices. A clean installation of the policy server cannot communicate with your EFW devices (this is the intended design, for security reasons).

If you do not create a backup diskette and you lose all Policy Server installation data, you will not be able to recover your EFW devices. They continue to enforce the fallback mode specified in their last EFW policy, indefinitely. These EFW devices must be replaced in order to obtain a different policy.

To backup your database using the Management Console, follow the steps below.

1. In the Main menu, select *Backup and Restore Database*.
2. Select *Backup*, and click *Next*.
3. Insert a blank diskette in the diskette drive.
4. Set the path location to the diskette drive (typically **a:\**) and specify the file name in the Path field.
5. If you want to password-protect the backup file, type a password in the Password field, and then retype the password in the Confirm field.

NOTE: The backup file contains EFW administrative passwords and cryptographic keys. Thus, the backup data should either be stored in a safe place, password-protected, or both.

NOTE: If you password-protect the backup data, make sure to record the password. The backup data cannot be accessed without the password.

6. Click *Next*. A summary window appears.
7. Click *Backup*. A confirmation window appears. Click *Finish*.
8. Remove, label, and secure the media.

Creating a No Sniffing Policy and Assigning it to the Default Device Set

In this section you will create a No Sniffing policy and assign it to the existing default device set.

A device set is a collection of EFW devices that are associated with a specific policy. You can define any number of device sets and assign EFW devices to any one of those device sets.

A policy is a set of criteria enforced by an EFW device. The No Sniffing policy prevents unauthorized access to network traffic (sniffing). This policy does not allow the EFW device to receive packets addressed to other firewall cards.

After this policy is assigned to the default device set, any EFW devices that automatically register with the Policy Server receive the No Sniffing policy because these EFW devices are automatically placed in the default device set upon registration. To register an EFW device simply means to add it to the Policy Server database.

To create the No Sniffing policy, follow the steps below.

1. In the Management Console, from the *Main* menu, select *New -> Policy*. The Create a New Policy window appears.
2. Enter *No Sniffing* for the policy name and click *Ok*. The Policy information window displays in the working frame.
3. Check the *No Sniffing* check box.
4. Click *Save.* The No Sniffing policy is created.

After you have created the No Sniffing policy, you can assign it to the default device set by following the steps below.

1. In the Management Console, click the *Device Sets* tab in the bottom left portion of the window.
2. Click *Default Device Set* in the tree-view frame. An information window for the default device set appears in the working frame.
3. Click the Policy drop-down list, and select *No Sniffing*.
4. Click *Save*. The No Sniffing policy is assigned to the default device set.

NOTE: You may assign any policy to the default device set. If you have a system that requires sniffing capabilities, you can manually register it and assign it to a device set with a different policy, or you can allow it to register with the system to the default device set and then move it to a different device set.

Installing and Registering an EFW device

Ensure the firewall card is installed using the installation CD delivered with the firewall card hardware, before proceeding with the following EFW device installation procedure. You are now ready to install and register an EFW device using the network installation method. You are about to configure a stationary EFW device, which has one policy.

NOTE: If diagnostics are desired for a firewall card installation, install them first from the installation CD delivered with the firewall card hardware, before installing EFW. Installing diagnostics over EFW may make the card inoperable.

NOTE: The EFW firmware has a tamper resistant design. Therefore, after installation of the firmware on a card, installing any non-EFW firmware over this EFW installation may render the card inoperable. If you wish to install non-EFW firmware on an EFW device, you must first successfully delete the device from its domain using the Management Console, as noted in the section "Uninstalling EFW" in the *3Com Embedded Firewall Administration Guide*.

1. In the Management Console *Tools* menu, select *Create FWC Installation*. The FWC Install Package wizard launches automatically.
2. Select *Network* as the installation package type and click *Next*.
3. From the drop-down list, select the first contact Policy Server for the EFW device installation when prompted. (This Policy Server is the one that you created during the installation process earlier in this guide.) Click *Next*.
4. Choose the location to which you want to save the installation information. (A network installation package is approximately 17 MB, therefore, it does not fit on a 3.5" diskette.) Click *Next*.
5. Review the information you entered, and click *Create* to create the installation package for the network. When prompted, click *Finish*.
6. Manually copy the contents of the folder specified in Step 4 to a temporary directory on the computer that will receive the FWC Install Package (on a computer on which the firewall card is installed).
7. On the computer receiving the FWC Install Package, run the setup.exe file located in the temporary directory that was copied in Step 6. (For larger installations of multiple EFW devices, you can simply run the installation from a login script or other installation utility.)
8. Follow the prompts. You may need to re-boot up to two times depending upon your Windows operating system.

Verifying EFW Device Registration

The EFW device automatically registers with the Policy Server on the final reboot that is required by the installation process. When the computer has finished rebooting, the EFW device is displayed in the Management Console. To verify that the EFW device registered correctly, follow the steps below.

1. In the Management Console, click the *Device Sets* tab in the lower left corner of the window.
2. Select *Edit -> Refresh*.
3. Click on the *Default Device Set* in the tree-view frame. Make sure *All Devices* is selected in the *Show* field. The EFW device should be listed in the default device set.
4. Double click on the entry for this device in the device set to view the device screen for this device.
5. Verify the following on the device screen:
   - On the Identification tab, ensure the *Last Wakeup or Heartbeat* time is recent.
   - On the Device Set tab, ensure the correct device set (*Default Device Set*) and policy (*No Sniffing*) are shown.
6. If desired, remove the temporary directory created for the EFW device installation package from the embedded firewall client machine. If you are going to continue on with this guide to try a roaming device installation on this same computer, do not remove it, as you will need it again.

For information on other installation methods, refer to the section “Distributing and Installing the EFW Firmware” in the *3Com Embedded Firewall Administration Guide*.

Changing the Policy for an EFW Device

You can allow all EFW Devices to register with the Default Device Set, and then move them to a different device set at a later time. To demonstrate such a move, you will:

- import a pre-defined rule set. A rule set is a group of packet filtering rules that can be reused in multiple policies.
- create a policy and add the new rule set
- assign the new policy to a device set
- test Internet access to ensure the system hosting the EFW device can reach the Internet

- move the EFW device to the device set
- test Internet access again to see that Internet access is no longer allowed

Importing the “Windows 2000 Standard” Rule Set

Before you create the sample policy, you need to import the Windows 2000 Standard rule set, which allows the system to boot up as a member of a Windows domain. This rule set will be added to the sample policy in the next section. The rule set was designed for Windows 2000, however, it may be used successfully on all Windows platforms supported by EFW.

To import the Windows 2000 Standard rule set, follow the steps below.

1. From the Main menu, select *Import Policy/Rule set*. The Import Policy/Rule Set window appears.
2. Select *Rule Set* and click *Next*.
3. Click *Browse* and navigate to *Program Files* -> *3Com Corporation* -> *3Com EFW* -> *predefined-policies-rulesets.xml*. Click *Choose*.
4. Click *Next*. A list of the rule sets contained in the file is displayed.
5. Select the *Windows 2000 Standard* pre-defined rule set and click *Next*. A summary window appears, showing the rule set you selected.
6. Click *Import*. A message appears indicating whether the import was successful.
7. Click *Finish*.

After you have imported the Windows 2000 Standard rule set, you can create a sample policy by following the steps in the section below.

Creating a Policy

In this section you will create a sample policy (called the “No IP Initiation” policy) that can be used on a system where the security goal is to minimize the threat to your network if the machine is taken over by a hostile external or internal agent. To achieve this goal, you will create a policy that:

- Allows the system to boot up as a member of a Windows domain (achieved by implementing the Windows 2000 Standard rule set in step 6 on the next page).
- Does not allow the system to initiate any TCP communication beyond that allowed to boot up and connect to the network domain, etc. This configuration prevents a hostile agent from using this machine as a

launching point for an attack on the network (achieved by the rule created in step 7 on the next page).

This type of policy would normally be used for a server machine. It is not appropriate for an end-user workstation or laptop because it would not allow the user to initiate any network traffic.

To create the "No IP Initiation" policy, follow the steps below.

1. In the Management Console *Main* menu, select *New* -> *Policy*. The Create a New Policy window appears.
2. Type *No IP Initiation* in the Policy field and click *OK*. The new policy information appears in the working frame.
3. Select the following policy-setting check boxes:
   - No Sniffing
   - Allow non-IP Traffic
   - Allow Fragmented IP Packets
   - Allow IP Options
4. Select *Last Policy (Block)* in the Fallback Mode drop-down list. Selecting this fallback mode means that if a stationary EFW device is unable to reach the Policy Server on boot up, it will enforce the last policy it received. If the EFW device is unable to load the last policy, the EFW device will allow no traffic except messages to and from the Policy Server and the DHCP, ARP, and 802.1x protocols.
5. Type a description of the policy in the Description field, if desired. This field is optional and exists solely to assist an administrator in assigning policies. You can include information about what the policy does, or when to use it (for example, the bulleted information provided at the beginning of this section).
6. The ACL initially contains only the default rule. Add the Windows 2000 Standard rule set as follows:

   a In the *Policy* menu, select *Rule Set* (or click the icon). The Rule Set Manager window appears.

   b Click on the *Windows 2000 Standard Rule Set* (that you imported in Importing the "Windows 2000 Standard" Rule Set on page 12) to select it, and then click *Add To Policy.*

   c Click *Close*. The rule set should appear in the ACL.
7. Create a "Deny outbound TCP SYN" rule as follows:

a In the *Policy* menu, select *Add Rule* (or click the icon). A new rule appears in the ACL.

b Click in the Rule Name cell, and type *Deny outbound TCP SYN*.

c Click in the Action cell, and select *Deny* from the drop-down list.

d Click in the Source IP Address cell, and select *EFW Device IP* from the drop-down list.

e Click in the IP Protocol cell, and select *tcp (6) init* from the drop-down list.

f Click in the Direction cell, and select *out* from the drop-down list.

g Click the check box in the Audit cell to enable audit.

You now have an effective "Deny outbound TCP SYN" rule. This rule should directly follow the Windows 2000 Standard rule set you added in step 6. If it does not, highlight the Deny outbound TCP SYN rule row, and use the arrow buttons to position it directly after the Windows 2000 Standard rule set.

8 Click *Save* to save the new policy information.

For more information on creating policies, refer to the section "Creating Policies and Rules" in the *3Com Embedded Firewall Administration Guide*.

Creating a Sample Device Set

Next you will create a sample device set whose member EFW devices will enforce the policy you created in the previous section.

To create the sample device set, follow the steps below.

1. From the *Main* menu, select *New* -> *Device Set*. The New Device Set window appears.
2. Type *Sample* in the Device Set Name field.
3. Select the *No IP Initiation* policy, which you created in the previous section, from the Policy for the New Device Set box.
4. Click *OK*. The device set information appears in the working frame.
5. Select a heartbeat interval of *15 minutes* from the Heartbeat drop-down list. (The heartbeat interval determines how often the EFW devices issue a heartbeat, or status update, to the Policy Server.)

6 Type *Sample device set enforcing the No IP Initiation policy* in the Description field. This field is optional and exists solely to assist an administrator in identifying the contents of the device set.

7 Click *Save*.

Moving the EFW Device to the New Device Set

Now that you have multiple device sets, you can move the EFW device from the default device set to the *No IP Initiation* device set that you created in the previous section by following the steps below.

1 Test your Internet access to ensure that the system hosting the EFW device can reach the Internet, for example, by connecting to *www.3com.com*. In a later section, you will attempt to access the Internet, which at that point should be denied by the policy being enforced.

2 In the Management Console, click the *Device Sets* tab in the tree-view frame.

3 Click *Default Device Set*. This device set contains the EFW device that you added earlier in this guide. In the working frame, ensure the *Show* menu is set to *All Devices*.

4 In the Device box, highlight the EFW device, and then click *Move*.

5 A list of alternative device sets appears. Select the *Sample* device set that you created in the previous section, and click *OK*. You will see a feedback window indicating that the new policy has been distributed to the embedded firewall. The EFW device is moved to the new device set and now enforces the new policy.

6 Click *Close.*

Testing Policy Enforcement and Viewing Audit Data

At this point you should have an EFW device enforcing the *No IP Initiation* policy. To ensure that the policy is functioning as expected, the following steps attempt to connect to the Internet by initiating the TCP protocol HTTP, which should be denied by the policy being enforced. You will then view the audit generated by the failed attempt.

1 On the machine hosting the EFW device, attempt to connect to *www.3com.com*. If you were denied access to the Internet, the EFW device is correctly enforcing the “No IP Initiation” policy. If you were able

to connect to the site, go back to the "Creating a Policy" section in this guide and verify that you correctly set up the policy rules.

2 To view the audit generated by this access attempt using the Management Console, follow the steps below:

- **a** In the *Audit* menu, select *Audit Browser* (or click the icon).
- **b** In the *Query* menu, select *New* (or click the icon). The Query Editor window appears.
- **c** Type *All Recent Audit Records* in the Query Name field.
- **d** In the Rule tab, select the *All Devices* check box in the For area, and the *All rule matches* check box in the Show area.
- **e** In the Policy tab, select the *All Policies* check box in the For area, and the *All policy events* check box in the Show area.
- **f** In the Administrator tab, select the *All administrator components* check box in the For area, and the *All administrator events* check box in the Show area.
- **g** Click *OK.*
- **h** In the Audit Browser window in the List of Queries, click on the *All Recent Audit Records* query you just created.
- **i** In the Query menu, select *Execute* (or click the icon).
- **j** Double-click on any event in the table to see detailed information for that event.

  The audit results should appear in table format. For information on viewing audit results, refer to the section "Audit Information" in the *3Com Embedded Firewall Administration Guide*.

Roaming EFW Device Configuration

If you are interested in using EFW on laptops that will have one policy inside the enterprise LAN (local) and another policy when outside the enterprise LAN (remote), complete the following roaming EFW device configuration example.

If you are new to EFW, complete all of the previous procedures to configure a firewall card as a stationary EFW device. This serves as a general introduction to EFW before proceeding. If you are familiar with EFW you may begin with this section to explore the new roaming feature in EFW 1.5.

The laptop EFW device models to use for this example are 3CRFW102 and 3CRFW103.

In this scenario, when the laptop is directly connected to the enterprise LAN, it will have a simple policy that will prohibit sniffing the network, and will prohibit access to one off limits enterprise server, but allow all other traffic to and from the laptop. This is called it's local policy.

When the laptop is connected to the enterprise LAN using a VPN, it will enforce a different policy called it's remote policy. The remote policy will allow only those protocols required for making a VPN connection to the enterprise network, and disallow any other traffic to or from any host on the Internet. In this example we are using the Microsoft PPTP VPN client. If you are not using the Microsoft PPTP VPN client, we will provide information to allow you to substitute policy rules appropriate for the VPN client you are using.

EFW provides a number of different ways a roaming EFW device determines its location. In this example the system will determine that the laptop is remote if it's connection to the Policy Server is through a VPN, and otherwise will determine that the laptop is operating locally.

This procedure will include the following:

- uninstall the EFW software from the stationary EFW device you configured in the previous sections, if you plan to reuse it for this section
- create local and remote policies
- create local and remote device sets
- create a locator, which specifies how an EFW device determines it's location
- install and register the roaming EFW device
- test local and remote policy enforcement

You do not normally need to uninstall the firewall card client software in order to change it from a stationary to roaming device. However, for the purpose of this guide, this method is used so you can see the full installation procedure for a roaming device.

Uninstall the EFW Software

If you have installed a laptop card as a stationary EFW device using the previous sections, do the following to uninstall EFW on this device if you wish to reuse it for your roaming example in the following sections.

1. Ensure the secured computer you want to uninstall is booted and live on the network that allows it to communicate with the Policy Server.
2. In the Management Console, click the *Policy Servers* tab in the lower left corner of the window.

3. Select *Edit -> Refresh Console.*
4. Right click anywhere in the tree-view frame and select *Expand Tree*.
5. Click *Network Interface Cards*.
6. In the working frame select the EFW device you want to delete.
7. In the Edit menu, select *Delete*. A confirmation window appears informing you that the EFW device will be deleted.
8. Click *OK*. The EFW device is removed from the EFW system and a command that disables the firewall functionality on the firewall card is sent to it.
9. Remove the EFW agent from the machine using the Windows Add/Remove program (*Start* -> *Settings* -> *Control Panel* -> *Add/Remove Programs*).
   - **a** Select *3Com Embedded Firewall*.
   - **b** Click *Add/Remove*.
   - **c** Click *Yes* to uninstall.

Create a Local Policy and Local Device Set

This scenario will have you modify and assign the No Sniffing policy to the local device set for your roaming device. This policy was created during the stationary EFW device installation procedure.

1. If you have not already created the No Sniffing policy, follow the procedure Creating a No Sniffing Policy and Assigning it to the Default Device Set on page 8.
2. Special tools are required to test the enforcement of the No Sniffing policy. You will add another rule to make it easier to verify that the local policy is being enforced. Identify any machine on your network with a static IP address to which you normally would not need connectivity. Use the following steps to add a rule that denies access from the laptop to this machine:
3. In the Management Console, click the *Policies* tab in the bottom left portion of the window.
4. Select *No Sniffing* the information window displays in the working frame.
5. Click rule wizard icon in the working frame.
   The rule description window appears in the working frame.

6 Type *Deny Specific IP* for a the rule name.

7 Click *Next*.

8 Select *Deny* from the Action drop-down.

9 Click *Next* twice.

10 Select *Host Name or IP Address* for the Destination IP Address drop-down and Enter the IP address identified above in the IP Address field.

11 Click *Next* three more times.

12 Click *Finish*.

13 Click *Save.*

Create a Remote Policy and Remote Device Set

This scenario will have you create a remote policy that supports the Windows native PPTP VPN Client. You will import the Windows 2000 PPTP pre-defined rule set used in this remote policy into the Management Console. Then you will create a remote device set whose member EFW devices will enforce the remote policy you created.

The remote policy for a roaming device is dependent on the type of VPN client used. If you want to try this exercise with a different VPN client, refer to the section “Creating Policies for VPN-Connected Telecommuters” in the *3Com Embedded Firewall Administrators Guide* to determine whether to use the following Windows 2000 IPSEC rule set instead of the Windows 2000 PPTP rule set in the following sections.

Importing the Windows 2000 PPTP Rule Set

In this section you will import a pre-defined rule set to use in your remote policy. To import the “Windows 2000 PPTP” pre-defined rule set, follow the steps below:

1 From the Management Console *Main* menu, select *Import Policy/Rule* set. The Import Policy/Rule Set window appears.

2 Select *Rule Set* and click *Next*.

3 Click *Browse* and navigate to *Program Files* -> *3Com Corporation* -> *3Com EFW* -> *predefined-policies-rulesets.xml*. Click *Choose*.

4 Click *Next*. A list of policies contained in the file appears.

5 Select the *Windows 2000 PPTP* pre-defined rule set and click *Next*. A summary window appears, showing the policy you selected.

Also, select the DNS client and DHCP client rule set if your laptop will need these services. If you do not know whether your laptop requires these services, add them to ensure the laptop has the needed connectivity for this exercise.

6 Click *Import*. A message appears indicating whether the import was successful.

7 Click *Finish*.

Create a Remote Policy

This example will have you create a policy that supports the Windows native PPTP VPN client. This policy only allows those protocols required by a Windows PPTP VPN client and does not allow protocols for browsing the web. This policy is intended for use by a VPN-connected mobile system where direct Web browsing is not allowed outside the VPN connection.

Use the following procedure to create a remote policy supporting the Windows native PPTP VPN client:

1 In the Management Console *Main* menu, select *New* -> *Policy*. The Create a New Policy window appears.

2 Type *PPTP VPN Only* for the name of the new policy and click *OK*. The new policy information appears in the working frame.

3 Select the Last Policy (Block) fallback mode from the Fallback Mode drop-down list.

Selecting this fallback mode means that if the EFW device is unable to reach the Policy Server on bootup it will enforce the last policy it received that is appropriate for its location (local or remote). If the device cannot determine its location or is unable to load the last policy, the EFW device will allow no traffic except messages to and from the Policy Server and the DHCP, ARP and 802.1x protocols.

4 Type a description of the policy in the *Description* field. This field is optional and exists solely to assist you in assigning policies. You can include information about what the policy does, or when to use it.

5 Select the *Policy* -> *Rule Set*. The Rule Set Manager dialog appears.

6 Select the *Windows 2000 PPTP* rule set from the rule set list.

Hold down the control key (to do a multiple select) and select *DNS client* and *DHCP client* if your laptop will need these services. If you do not know whether your laptop requires these services, add them to ensure the laptop has the needed connectivity for this exercise.

7 Click *Add to Policy*.

8 Click *Close*. The rule sets you selected are added to the policy.

9 Click *Save*. The PPTP VPN Only policy is created.

Create a Remote Device Set

Next you will create a remote device set whose member EFW devices will enforce the policy you created in the previous section.

1 Click the *Device Sets* tab.

2 Click *Device Set* in the tree-view frame.

3 From the Main menu, select *New -> Device Set.*

4 Enter *VPN-Connected* for the Device Set Name.

5 From the *Policy for the new device set* window, select the *PPTP VPN Only* policy.

6 Click *OK*.

Creating a Locator

A locator is a set of criteria that determines where the roaming EFW device is, so the system can give the device the correct policy.

The network configuration of your organization will determine which type of locator will best distinguish local and remote operations of the roaming systems you plan to secure with EFW. For this example we use a method that will be appropriate for many organizations. See *3Com Embedded Firewall Administration Guide* for other supported methods.

To create a locator, follow the steps below:

1 From the Main menu, select *New -> Locator*. The New Locator window appears.

2 Type *VPN-Connection* in the Locator Name field.

3 Select the local Device Set that you want to associate with this locator from the Local Device Set drop down list. Devices in this locator will simply inherit this local device set unless you explicitly select other local device sets for them. For the Local Device Set, leave the *Default Device Set* selection.

4 From the Remote Device Set drop down list select the *VPN-Connected* Device Set that you created earlier.

5 Click *OK*. The locator screen appears, it is split into three tab-accessible panels; Identification, Location Criteria, and Device Sets. You should be in the Identification panel.

6 Select the *Location Criteria* tab.

7 Select the *Non-VPN connection to Policy Server* radio button.

8 Make sure the *Remote* radio button is selected.

9 Click the *Registration Criteria* button.

10 Click the *IP Address Mask* radio button.

11 Enter an IP address and mask that the laptop will match when operating locally on the LAN. For example if the laptop operates on the LAN with an IP of *192.168.1.6* enter *192.168.1.0*, and an IP Address Mask of *255.255.255.0*. This setting has the effect that if any mobile EFW device on the network 192.168.1 automatically registers with the Policy Server, it will be placed in the VPN-Connection locator.

12 Click *OK*.

13 Click *Save*. The locator is now configured.

Installing and Registering a Roaming EFW Device

To configure the roaming EFW device you must be directly connected to your enterprise LAN.

1 Before installing the EFW client, make sure you can ping the machine you selected above that will later become off limits to your laptop on the enterprise LAN.

2 You are now ready to install and register the roaming EFW device using the network installation method. Follow steps 1 through 7 of Installing and Registering an EFW device on page 9. However, if you already have the network install package copied to the laptop, simply follow step 7 of Installing and Registering an EFW device on page 9.

Verifying EFW device Registration

The EFW device automatically registers with the Policy Server on the final reboot that is required by the installation process. When the computer has finished rebooting, the EFW device is displayed in the Management Console. To verify that the EFW device registered correctly, follow the steps below.

1. In the Management Console, click the *Device Sets* tab in the lower left corner of the window.
2. Right click anywhere in the tree-view frame and select *Expand Tree* to expand the tree in the tree-view frame. In the expanded *Default Device Set*, your roaming device should appear as *Roaming Local (1)*, and in the *VPN-Connected* device set should appear as *Roaming Remote (1)*.

   In addition, you can verify EFW device registration using the following procedure:

   a Click the *Locators* tab in the lower left corner of the window.

   b Click on *VPN-Connection* to show the VPN-Connection locator in the right frame.

   c Click on the Device Sets tab. You will see your device listed in the locator.
3. Double click your device in the Devices list. This will display the screen for this device in the working frame.
4. Verify the following:
   - On the Identification tab, ensure the *Last Wakeup or Heartbeat* time is recent.
   - On the Device Set tab, ensure the correct local (*Default Device Set* with *No Sniffing* policy) and remote device sets and policy (*VPN-Connected* device set with *PPTP VPN Only* policy) are shown.
5. If desired, remove the temporary directory created for the EFW device installation package from the embedded firewall client machine.

For information on other installation methods, refer to the section “Distributing and Installing the EFW Firmware” in the *3Com Embedded Firewall Administration Guide*.

Testing the Roaming EFW Policies

At this point you should have the roaming EFW device enforcing the enhanced *No Sniffing* policy for local connection, and the *PPTP VPN Only* policy for remote connection.

1. To ensure the local policy is functioning as expected, while directly connected to the enterprise LAN, attempt to **`ping`** the IP address entered in the Deny Specific IP rule created for the local policy in the step 10 of the

Create a Local Policy and Local Device Set section. This attempt should timeout.

2 To test your remote policy first you must connect to your enterprise network via your VPN. To show your laptop is operating remotely and enforcing the remote policy, try one of the following:

- Try to **`ping`** any machine outside your enterprise network.
- From another machine outside your enterprise network, attempt to **`ping`** your machine.
- Attempt to browse the internet directly through an Internet Service Provider and not via the VPN client.

All of these connection attempts should fail. View audit for these attempts when you again have access to the Management Console. See step 2 of Testing Policy Enforcement and Viewing Audit Data on page 15.

Expanding Your EFW Configuration

Now that you have a basic EFW system configured and running, you can expand your configuration as needed to best suit your organization's security needs. The following list provides some sectional references to the *3Com Embedded Firewall Administration Guide* that will assist you in expanding your configuration.

- For an overview of EFW and its basic components, concepts, and operations, refer to Chapter 1, "Planning and Overview."
- To install additional remote Management Consoles, refer to Chapter 2, "Installing and Uninstalling EFW Software."
- To add additional EFW devices to your system, refer to Chapter 2, "Distributing and Installing the EFW Firmware."
- To add additional Policy Servers for redundancy, refer to Chapter 3, "Configuring Policy Servers for Redundancy."
- For information on methods of detecting roaming device locations, refer to Chapter 3, "Creating a Locator."
- To create additional policies, refer to Chapter 4, "Creating Policies and Rules."